REMARKS/ARGUMENTS

Prior to this Amendment, claims 1-8, 10-17, 19-26, 28-38 and 41-42 were pending. In this Amendment, claims 1, 8, 10, 19, and 34 are amended, claims 43-44 are added, and no claims are canceled, so that claims 1-8, 10-17, 19-26, 28-38, and 41-44 are pending.

I. Examiner Interview

On November 18, 2008, applicants' representative P. Jewik conducted an in-person interview with Examiner Worjloh. The undersigned also participated in the interview via telephone. Examiner Worjloh is sincerely and earnestly thanked for her consideration of the arguments made by the applicants' representatives.

During the interview, the claims were discussed in light of the cited references. In this amendment, each of the independent claims is amended to include additional limitations. Support for the amendments can be found throughout the specification and figures, including places such as paragraphs 18, 34, 42, and 43. During the interview the examiner suggested that the claims be amended to clarify the message routing between the various participants in the system. The claims have been amended to incorporate the Examiner's suggestion. Applicants' representative believes that such amendments would move this application closer to allowance.

II. Brief Summary

In order to assist in the examination of the claims, a brief summary of the present application may be helpful. Some embodiments of the present application relate to the field of authenticating users conducting transactions online. It should be noted that authentication is the process of verifying a user is who he actually claims to be, whereas a payment process is the process of actually transferring funds from one entity to another. Although a payment process may follow an authentication process, the two processes are not synonymous. The following description may be more easily understood in conjunction with Figure 2 of the application. The numbers in parenthesis indicate elements within Figure 2.

In one exemplary embodiment of the present application, a cardholder may purchase goods or services from an e-commerce merchant's web site (210) using a credit card. The merchant may authenticate the cardholder by sending a request for authentication to a central transaction server (252/272). The central transaction server (280) may send a response to the merchant that instructs the merchant to redirect the user to the central transaction server (274/258). The response may also include a pseudonym that the merchant passes (260) to the cardholder (205) and may be sent to the central transaction server (280) after the cardholder has been redirected (260). The pseudonym may be used to correlate various messages and responses, as will become clear later. The redirection request may also include transaction information that may further assist in the authentication process.

The central transaction server may then be contacted by the redirected cardholder (262). The cardholder may provide the central transaction server with the pseudonym and the transaction information. Based on the pseudonym, the central transaction server may determine the access control server (225) that is providing authentication services for the issuer of the cardholder's credit card. It should be noted that every credit card issuer (e.g. Citibank, Chase, Wells Fargo) may have its own access control server. Once the proper access control server has been determined, the central transaction server may send a request (270) to the access control server to authenticate the cardholder. The request may include the pseudonym.

The central transaction server may then relay (276/270) authentication information between the cardholder and the access control server. The pseudonym may be used to correlate the messages passed between the access control server and the cardholder. The central transaction server may process requests for any number of cardholders, and the pseudonym may be used to correctly route the authentication information to the correct cardholder. Once the access control server has authenticated the cardholder, such as by requesting a password, the access control server may send a response (266) to the central transaction server indicating the cardholder has been authenticated. The central transaction server may send a response (278) to the cardholder, the response redirecting (268) the cardholder back to the merchant system. The response may also include an indication that the cardholder has been authenticated. The pseudonym may also be included to correlate the messages.

The cardholder who has now been redirected back to the merchant may present the authentication indication and the pseudonym to the merchant to demonstrate that the cardholder has been authenticated. The pseudonym may be used to confirm to the merchant that the original authentication request from the merchant corresponds to the authentication response that is now being received. One way this may be accomplished is by requiring the pseudonym to expire after a predetermined period of time. If an authentication response is received for an expired pseudonym, the response may be ignored. This may prevent a fraudulent user from intercepting and reusing an authentication response for additional transactions at a later time.

Once the cardholder has been authenticated, a payment process may be initiated. The payment process may proceed using the cardholder's actual account number, with the merchant sending the account number to a card acquirer for further processing of the payment.

III. Rejections

In the Office Action mailed on September 25, 2008, a number of rejections are made. They are as follows:

1. Claims 1, 2, 7, 8, 10, 11, 16, 17, 19, 20, 25, 26, 32, 33, 38, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Publication No. 2005/0021781 to Sunder et al. ("*Sunder*") in view of U.S. Publication No. 2004/0158532 to Breck et al. ("*Breck*").

2. Claims 3, 12, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Publication No. 2005/0021781 to Sunder et al. ("*Sunder*") in view of US Publication No. 2004/0158532 to Breck et al. ("*Breck*") in further view of U.S. Publication No. 2003/0046541 to Gerdes et al. ("*Gerdes").*

3. Claims 4-6, 13-15, 22-24 and 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Publication No. 2005/0021781 to Sunder et al. ("*Sunder*") in view of US Publication No. 2004/0158532 to Breck et al. ("*Breck*") in further view of U.S. Publication No. 2004/0254848 to Golan et al. ("*Golan").*

4. Claims 34-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Publication No. 2005/0021781 to Sunder et al. ("*Sunder*") in view of US Publication No. 2004/0158532 to Breck et al. ("*Breck*") in further view of U.S. Publication No. 2004/0254848 to Golan et al. ("*Golan").*

Each of the above rejections is traversed. None of the cited references teaches or suggests, *inter alia*, "wherein the authentication response includes a second HTTP redirect command comprising the address of the merchant, wherein the cardholder system forwards the authentication response to the merchant system" as recited in independent claim 1. At best, *Breck* may describe a cardholder system being redirected to a card issuer system to receive an STN (e.g. pseudonym), but *Breck* does not describe a second HTTP redirect command to redirect the cardholder system back to the merchant system after receiving an authentication response.

Additionally, none of the cited references teach or suggest "wherein the pseudonym is used for authentication" as recited in claim 1. At best, *Breck* teaches an STN which may describe a one time or limited time use account number that is used for payment authorization.

Furthermore, none of the cited references teach or suggest a merchant system "wherein the merchant system analyzes the authentication response to determine if the electronic commerce card account number has been successfully authenticated and initiates a payment request process by submitting the electronic commerce card account number to the issuer of the electronic commerce card account number" as recited in claim 1. *Sunder* does not describe initiating a payment request as admitted in the office action. *Breck* at best describes initiating a payment process from a merchant using the STN, which is purposefully not the same as the electronic commerce card account number, as the purpose of the STN is to not expose the real account number to the merchant.

The remaining independent claims recite at least some limitations that are similar to those presented in amended claim 1 and are allowable for at least some of the same reasons as set forth above. Furthermore, the remaining dependent claims are allowable at least by virtue of their dependence from their corresponding independent claim. Withdrawal of these rejections is respectfully requested.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

/Preetam B. Pagar/

Preetam B. Pagar
Reg. No. 57,684

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
PBP:scz
61716855 v1